Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 858–864
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Hilbert–Speiser number fields for a prime p inside the p-cyclotomic field

Humio Ichimura

Faculty of Science, Ibaraki University, Bunkyo 2-1-1, Mito, 310-8512, Japan

Received 17 September 2006; revised 3 December 2006

Available online 2 October 2007

Communicated by David Goss

Abstract

Let p be a prime number. We say that a number field F satisfies the condition (H'_p) when for any cyclic extension N/F of degree p, the ring $\mathcal{O}'_N$ of p-integers of N has a normal integral basis over $\mathcal{O}'_F$. It is known that $F = \boldsymbol{Q}$ satisfies (H'_p) for any p. It is also known that when $p \leqslant 19$, any subfield F of $\boldsymbol{Q}(\zeta_p)$ satisfies (H'_p). In this paper, we prove that when $p \geqslant 23$, an imaginary subfield F of $\boldsymbol{Q}(\zeta_p)$ satisfies (H'_p) if and only if $F = \boldsymbol{Q}(\sqrt{-p})$ and $p = 43$, 67 or 163 (under GRH). For a real subfield F of $\boldsymbol{Q}(\zeta_p)$ with $F \neq \boldsymbol{Q}$, we give a corresponding but weaker assertion to the effect that it quite rarely satisfies (H'_p).

MSC: 11R18; 11R33; 11R23

1. Introduction

Let p be a *fixed* prime number and F a number field. Let $\mathcal{O}_F$ be the ring of integers of F, and $\mathcal{O}'_F = \mathcal{O}_F[1/p]$ the ring of p-integers. Let h_F and h'_F be the class numbers of the Dedekind domains $\mathcal{O}_F$ and $\mathcal{O}'_F$, respectively. Let Γ be the cyclic group of order p. A Γ-extension N/F has a normal p-integral basis (p-NIB for short) when $\mathcal{O}'_N$ is cyclic over the group ring $\mathcal{O}'_F[\Gamma]$. We say that F satisfies the condition (H'_p) when any Γ-extension over F has a p-NIB. It is known that the rationals $\boldsymbol{Q}$ satisfy (H'_p) for all p. This is essentially due to Hilbert and Speiser. Let $K = F(\zeta_p)$. It is known that F satisfies (H'_p) if $h'_K = 1$ ([2, Theorem] or [3, Theorem 1]).

E-mail address: hichimur@mx.ibaraki.ac.jp.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.06.007

Let p be an odd prime number. Let $K = \boldsymbol{Q}(\zeta_p)$, and $h_p = h_K$. As the unique prime ideal of $\mathcal{O}_K$ over p is principal, we have $h_p = h'_K$. It is known that $h_p = 1$ if and only if $p \leqslant 19$ (cf. Washington [12, Theorem 11.1]). Therefore, when $p \leqslant 19$, any subfield F of K satisfies (H'_p) by the above mentioned result [2, Theorem]. When $p \geqslant 23$, we proposed the following conjecture in [5].

Conjecture. *Let $p \geqslant 23$ be a prime number, and let F be a subfield of $K = \boldsymbol{Q}(\zeta_p)$ with $F \neq \boldsymbol{Q}$. If $[F : \boldsymbol{Q}] > 2$ or $p \equiv 1 \bmod 4$, then F does not satisfy the condition (H'_p) except for the case where $p = 29$ and $[F : \boldsymbol{Q}] = 2$ or 7.*

In [5, Proposition 4], we showed that when $23 \leqslant p \leqslant 499$, this assertion is valid for any F, and that it is valid for any $p \geqslant 23$ if $[K : F] \leqslant 4$ or $[K : F] = 6$. We also showed that when $p = 29$ and $[F : \boldsymbol{Q}] = 2$ or 7, F satisfies (H'_p). When $p \equiv 3 \bmod 4$ and $F = \boldsymbol{Q}(\sqrt{-p})$ is the quadratic subfield of $\boldsymbol{Q}(\zeta_p)$, we only showed that F satisfies (H'_p) when $p = 43$ or 67 [5, Remark 2].

The purpose of this paper is to give an answer to the conjecture including the case where $p \equiv 3 \bmod 4$ and $F = \boldsymbol{Q}(\sqrt{-p})$. We prove the following:

Theorem 1. *Let p be a prime number with $p \geqslant 23$, and $K = \boldsymbol{Q}(\zeta_p)$.*

(I) *An imaginary subfield F contained in K does not satisfy the condition (H'_p) except for the case where $F = \boldsymbol{Q}(\sqrt{-p})$ and $p = 43$, 67 or 163.*
(II) *Let $F = \boldsymbol{Q}(\sqrt{-p})$. When $p = 43$ or 67, F satisfies (H'_p). When $p = 163$, F satisfies (H'_p) under GRH.*

For the real case, we prove the following weaker result. Let h_p^- be the relative class number of $\boldsymbol{Q}(\zeta_p)$. Assume that a prime number p satisfies the condition:

(C) there exists a prime factor q of h_p^- with $q \nmid p - 1$.

Under this assumption, let D_p be the smallest value of $\operatorname{ord}_q(h_p^-)$ for all prime factors q of h_p^- with $q \nmid p - 1$. By the table [13] of Yamamura on h_p^-, we see that for any prime number p with $23 \leqslant p \leqslant 1021$, the condition (C) is satisfied except for the case where $p = 29$ or 31. For these p with $p \neq 29, 31$, we have $D_p = 1$ when $p \neq 41$ and $D_p = 2$ when $p = 41$. (We have $h_{29}^- = 8$, $h_{31}^- = 9$ and $h_{41}^- = 11^2$.) It is plausible that (C) is satisfied and $D_p = 1$ for all $p \geqslant 23$ with the above exceptions.

Theorem 2. *Let $p \geqslant 23$ be a prime number satisfying the condition* (C)*, and let $K = \boldsymbol{Q}(\zeta_p)$. A real subfield F of K does not satisfy (H'_p) when $[F : \boldsymbol{Q}] > D_p$.*

From this theorem and [5, Proposition 4] mentioned above, it follows that a real subfield $F \neq \boldsymbol{Q}$ of $K = \boldsymbol{Q}(\zeta_p)$ does not satisfy (H'_p) for $23 \leqslant p \leqslant 1021$ except for the case where $p = 29$ and $[F : \boldsymbol{Q}] = 2$ or 7.

2. Stickelberger ideals of conductor p

In this section, we recall some results in [3] and [5] on Stickelberger ideals of conductor p, which are necessary to prove Theorems 1 and 2. Let p be a *fixed* odd prime number, and let

$G = (\boldsymbol{Z}/p)^\times$ be the multiplicative group. Let $\mathcal{S}_G$ be the classical Stickelberger ideal of the group ring $\boldsymbol{Z}[G]$ associated to the abelian extension $\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}$. For an integer $i \in \boldsymbol{Z}$ with $p \nmid i$, let $\sigma_i = \bar{i}$ be the corresponding element of G. For an integer $r \in \boldsymbol{Z}$, let

$$\theta_r = \sum_{i=1}^{p-1} \left[\frac{ri}{p}\right] \sigma_i^{-1} \in \boldsymbol{Z}[G],$$

where for a real number x, $[x]$ denotes the largest integer $\leqslant x$. It is known that $\mathcal{S}_G$ is generated by Stickelberger elements θ_r for all r over $\boldsymbol{Z}$ (cf. [12, Lemma 6.9]).

Let H be a subgroup of G. For an element $\alpha \in \boldsymbol{Z}[G]$, we write

$$\alpha_H = \sum_{\sigma \in H} a_\sigma \sigma \quad \text{with } \alpha = \sum_{\sigma \in G} a_\sigma \sigma. \tag{1}$$

Namely, α_H is an "H-part" of α. In [3–5], we defined a Stickelberger ideal $\mathcal{S}_H$ of $\boldsymbol{Z}[H]$ by

$$\mathcal{S}_H = \{\alpha_H \mid \alpha \in \mathcal{S}_G\},$$

and studied some of its properties. For brevity, let $\theta_{r,H} = (\theta_r)_H$. As $\mathcal{S}_G$ is generated by the elements θ_r over $\boldsymbol{Z}$, the H-part $\mathcal{S}_H$ is generated by $\theta_{r,H}$ over $\boldsymbol{Z}$ for all r. We can easily show that

$$\sigma_s \theta_{r,H} = \theta_{rs,H} - r\theta_{s,H} \quad \text{for } \bar{s} \in H. \tag{2}$$

For this, see [3, Section 2]. Further, we can show the following formula [5, Lemma 3]

$$\mathcal{S}_G \subseteq \mathcal{S}_H \boldsymbol{Z}[G]. \tag{3}$$

Let F be a number field. Let Cl_F and Cl'_F be the ideal class groups of the Dedekind domains $\mathcal{O}_F$ and $\mathcal{O}'_F = \mathcal{O}_F[1/p]$, respectively. Letting D be the subgroup of Cl_F generated by the classes containing a prime ideal of $\mathcal{O}_F$ over p, Cl'_F is naturally isomorphic to Cl_F/D. Hence, when primes of $\mathcal{O}_F$ over p are principal, we have $Cl'_F = Cl_F$. Let $K = F(\zeta_p)$, and $H = \mathrm{Gal}(K/F)$. We regard H as a subgroup of G through the Galois action on ζ_p. In [5, Appendix], we showed the following assertion using the main theorem of McCulloh [10]. A direct and simpler proof is given in [3] (see Remark 1).

Theorem 3. *Let F be a number field. Let $K = F(\zeta_p)$ and $H = \mathrm{Gal}(K/F) \subseteq G$. Then, F satisfies the condition (H'_p) if and only if the Stickelberger ideal $\mathcal{S}_H$ annihilates the class group Cl'_K.*

The following is a consequence of Theorem 3.

Lemma 1. *(See [3, Corollary 4].) Under the setting of Theorem* 3*, assume that the norm map $Cl'_K \to Cl'_F$ is surjective. Then, F satisfies (H'_p) only when the natural map $Cl'_F \to Cl'_K$ is trivial.*

Remark 1. In [3], we showed an assertion stronger than Theorem 3. Under the setting of Theorem 3, we showed that if $\mathcal{S}_H$ annihilates Cl'_K, then any abelian extension N/F of exponent p has a p-NIB.

3. Proof of Theorem 2

To show Theorem 2, we first introduce some notation. We *fix* a prime number q with $q \nmid p-1$. Let $\boldsymbol{Q}_q$ be the field of q-adic rationals, and $\boldsymbol{Z}_q$ the ring of q-adic integers. Let Ψ be a $\boldsymbol{Q}_q$-valued character of $G = (\boldsymbol{Z}/p)^\times$ defined and irreducible over $\boldsymbol{Q}_q$. For simplicity, we call such a character a $\boldsymbol{Q}_q$-character of G. Let ψ be an irreducible component of Ψ over $\bar{\boldsymbol{Q}}_q$ where $\bar{\boldsymbol{Q}}_q$ is an algebraic closure of $\boldsymbol{Q}_q$. Then, Ψ is the sum of characters of G which are conjugate to ψ over $\boldsymbol{Q}_q$. Let H be a subgroup of G. Let ψ_H be the restriction of ψ to H, and let Ψ_H be the $\boldsymbol{Q}_q$-character of H having ψ_H as an irreducible component over $\bar{\boldsymbol{Q}}_q$. For a module M over $\boldsymbol{Z}[G]$ and a $\boldsymbol{Q}_q$-character Ψ of G, let $M(\Psi)$ be the Ψ-component of the q-part $M \otimes \boldsymbol{Z}_q$ of M. Then, as $q \nmid p-1$, $M \otimes \boldsymbol{Z}_q$ is canonically decomposed as

$$M \otimes \boldsymbol{Z}_q = \bigoplus_{\Psi} M(\Psi)$$

where Ψ runs over the $\boldsymbol{Q}_q$-characters of G. We have a similar decomposition for a module over $\boldsymbol{Z}[H]$. Let ψ be an irreducible component over $\bar{\boldsymbol{Q}}_q$ of a $\boldsymbol{Q}_q$-character Ψ. Let $\boldsymbol{Z}_q[\psi]$ (respectively $\boldsymbol{Z}_q[\psi_H]$) be the subring of $\bar{\boldsymbol{Q}}_q$ generated by the values of ψ (respectively ψ_H) over $\boldsymbol{Z}_q$. Sending an element $\sigma \in G$ to $\psi(\sigma)$, we have natural ring isomorphisms

$$\psi : \boldsymbol{Z}_q[G](\Psi) \cong \boldsymbol{Z}_q[\psi] \quad \text{and} \quad \psi_H : \boldsymbol{Z}_q[H](\Psi_H) \cong \boldsymbol{Z}_q[\psi_H].$$

A module M over $\boldsymbol{Z}[G]$ is naturally regarded also as a $\boldsymbol{Z}[H]$-module. By the above isomorphism, we can regard the component $M(\Psi)$ (respectively $M(\Psi_H)$) of M as a module over $\boldsymbol{Z}_q[\psi]$ (respectively $\boldsymbol{Z}_q[\psi_H]$). In particular, for an ideal $\mathfrak{A}$ of $\boldsymbol{Z}_q[H]$, we have

$$M(\Psi_H)^{\mathfrak{A}} = M(\Psi_H)^{\psi_H(\mathfrak{A})}.$$

For simplicity, we put

$$\mathcal{S}_{G,q} = \mathcal{S}_G \otimes \boldsymbol{Z}_q \quad \text{and} \quad \mathcal{S}_{H,q} = \mathcal{S}_H \otimes \boldsymbol{Z}_q.$$

Proof of Theorem 2. Let q be a prime factor of h_p^- with $q \nmid p-1$, and $D = \operatorname{ord}_q(h_p^-)$. Let $K = \boldsymbol{Q}(\zeta_p)$. We have $Cl_K = Cl'_K$ as the unique prime ideal of $\mathcal{O}_K$ over p is principal. Let F be a real subfield of K with $[F : \boldsymbol{Q}] > D$, and let $H = \operatorname{Gal}(K/F)$. Through the Galois action on ζ_p, we identify the Galois group $\operatorname{Gal}(K/\boldsymbol{Q})$ with $G = (\boldsymbol{Z}/p)^\times$, and H with a subgroup of G. Thus, we can regard the class group $Cl'_K = Cl_K$ not only as a $\boldsymbol{Z}[H]$-module but also as a module over $\boldsymbol{Z}[G]$. As $D = \operatorname{ord}_q(h_p^-)$, there exist at most D odd $\bar{\boldsymbol{Q}}_q$-valued irreducible characters ϕ of G with $q \mid B_{1,\phi^{-1}}$ by the analytic class number formula [12, Theorem 4.17]. We fix one of such characters ϕ. Let Φ be the $\boldsymbol{Q}_q$-character of G having ϕ as an irreducible component over $\bar{\boldsymbol{Q}}_q$. As F is real, the complex conjugation σ_{-1} is contained in H. Therefore, since $[G : H] = [F : \boldsymbol{Q}] > D$, there exists an *odd* $\bar{\boldsymbol{Q}}_q$-valued character ψ of G such that $\psi_H = \phi_H$ and $q \nmid B_{1,\psi^{-1}}$. Let Ψ be the $\boldsymbol{Q}_q$-character of G having ψ as an irreducible component over $\bar{\boldsymbol{Q}}_q$. As $q \nmid B_{1,\psi^{-1}}$, we see that $\psi(\mathcal{S}_{G,q}) = \boldsymbol{Z}_q[\psi]$. Hence, by (3), it follows that $\psi_H(\mathcal{S}_{H,q}) = \boldsymbol{Z}_q[\psi_H]$. Therefore, we obtain

$$Cl_K(\Psi_H)^{\mathcal{S}_{H,q}} = Cl_K(\Psi_H)^{\psi_H(\mathcal{S}_{H,q})} = Cl_K(\Psi_H).$$

On the other hand, as $\psi_H = \phi_H$, we have $Cl_K(\Psi_H) = Cl_K(\Phi_H)$. The Φ-component $Cl_K(\Phi)$ of the $\boldsymbol{Z}[G]$-module Cl_K is a direct summand of the Φ_H-component $Cl_K(\Phi_H)$ of the $\boldsymbol{Z}[H]$-module Cl_K. As $q \mid B_{1,\phi^{-1}}$, we see that $Cl_K(\Phi)$ is nontrivial by the theorem of Mazur and Wiles [9] (Iwasawa main conjecture). Therefore, $Cl_K^{S_H}$ is nontrivial, and hence, F does not satisfy (H'_p) by Theorem 3. □

Remark 2. For an imaginary subfield F of $K = \boldsymbol{Q}(\zeta_p)$ with $[F : \boldsymbol{Q}] > 2D_p$, we can show a similar assertion by a similar argument.

4. Proof of Theorem 1

4.1. CM-fields

For a number field F, let W_F be the group of roots of unity in F. For a CM-field F, let Cl_F^- be the kernel of the norm map $Cl_F \to Cl_{F^+}$ where F^+ is the maximal real subfield of F. The following lemma is a generalization of a well-known assertion on the cyclotomic $\boldsymbol{Z}_p$-extension over a CM-field [12, Proposition 13.26], and is more or less known to specialists. For a finite abelian group A and a prime number q, let $A(q)$ be the Sylow q-subgroup of A.

Lemma 2. *Let q be an odd prime number. Let E/F be a cyclic extension of degree q with both E and F CM-fields. Assume that $W_F(q) = \{0\}$ or $|W_E(q)/W_F(q)| > 1$. Then, the natural map $Cl_F^-(q) \to Cl_E$ is injective.*

Outline of proof. The proof of this lemma goes through exactly similarly to the argument in [12, pp. 288–290]. So, we only give an outline of the proof. Let σ be a generator of the cyclic group $\mathrm{Gal}(E/F)$ of order q, and let J be the complex conjugation of E. Let $\mathfrak{A}$ be an ideal of $\mathcal{O}_F$ such that $[\mathfrak{A}]_F \in Cl_F^-(q)$ and $\mathfrak{A}\mathcal{O}_E = \alpha\mathcal{O}_E$ for some $\alpha \in \mathcal{O}_E$. Here, $[\mathfrak{A}]_F$ is the ideal class in Cl_F represented by $\mathfrak{A}$. As $\mathfrak{A}$ is an ideal of F, we have $\alpha^{\sigma-1} = \epsilon$ for some unit $\epsilon \in \mathcal{O}_E^\times$. As $[\mathfrak{A}]_F \in Cl_F^-$, we have $\mathfrak{A}^{1+J} = \beta\mathcal{O}_F$ for some $\beta \in F^\times$. Hence, it follows that $\alpha^{1+J} = \beta\eta$ for some $\eta \in \mathcal{O}_E^\times$, and that

$$\epsilon^{1+J} = \alpha^{(1+J)(\sigma-1)} = \eta^{\sigma-1} \tag{4}$$

as $\beta \in F^\times$. Let $\alpha_1 = \alpha^2/\eta$ and let

$$\epsilon_1 = \alpha_1^{\sigma-1} = \frac{\epsilon^2}{\eta^{\sigma-1}} \in \mathcal{O}_E^\times.$$

We see from (4) that

$$\epsilon_1^{1+J} = \epsilon^{2(1+J)}\eta^{(1-\sigma)(1+J)} = \eta^{(\sigma-1)(1-J)}.$$

As E is a CM-field, it follows that $\epsilon_1 \in W_E$ from a theorem on units of a CM-field (cf. [12, Theorem 4.12]). On the other hand, we have

$$N(\epsilon_1) = N\bigl(\alpha_1^{\sigma-1}\bigr) = 1,$$

where N is the norm map from E to F. Under the assumption that $W_F(q) = \{0\}$ or $|W_E(q)/W_F(q)| > 1$, we can show that the first cohomology group $H^1(E/F, W_E)$ is trivial exactly similarly to the proof of [12, Lemma 13.27]. Therefore, $\epsilon_1 = \zeta^{\sigma-1}$ for some $\zeta \in W_E$. It follows that $(\alpha_1/\zeta)^\sigma = \alpha_1/\zeta$, and $\alpha_1/\zeta \in F^\times$. This implies that the ideal $\mathfrak{A}^2$ of $\mathcal{O}_F$ is principal. As the order of the class $[\mathfrak{A}]_F$ is odd, we obtain $[\mathfrak{A}]_F = 1$. □

The following lemma is well known.

Lemma 3. *Let E/F be a finite extension of a number field F, and let q be a prime number with $q \nmid [E : F]$. Then, the natural map $Cl_F(q) \to Cl_E$ is injective.*

4.2. Proof of Theorem 1

Let p be a prime number with $p \geqslant 23$, and let $K = \boldsymbol{Q}(\zeta_p)$. As $h_p > 1$, we see that K does not satisfy (H'_p) by Theorem 3 (or [3, Corollary 1]). Let F be an imaginary proper subfield of K. As the unique prime ideal of $\mathcal{O}_F$ over p is principal, we have $Cl_F = Cl'_F$ and $h_F = h'_F$. Let $h_F^- = |Cl_F^-|$ be the relative class number of F. If h_F^- is not a power of 2, then it follows from Lemmas 2 and 3 that the natural map $Cl_F^- \to Cl_K$ is not trivial. Hence, it follows from Lemma 1 that F does not satisfy (H'_p).

Horie [1] proved that there are only finitely many pairs (p, F) for which h_F^- is a power of 2, and that the relative class number h_p^- of $\boldsymbol{Q}(\zeta_p)$ is a power of 2 if and only if ($p \leqslant 19$ or) $p = 29$. In [8, Theorem 7], Louboutin proved that for an imaginary proper subfield F of $\boldsymbol{Q}(\zeta_p)$ with $p \geqslant 23$, h_F^- is a power of 2 if and only if

$$\begin{aligned}\big(p, [F : \boldsymbol{Q}]\big) = {} & (29, 4),\ (37, 4),\ (37, 12),\ (41, 8),\ (43, 2),\ (43, 6),\ (43, 14),\\ & (53, 4),\ (61, 4), (61, 12), (67, 2),\ (67, 6), (163, 2) \text{ or } (163, 6).\end{aligned}$$

By the numerical result [5, Proposition 4], the Conjecture in Section 1 is valid for p with $23 \leqslant p \leqslant 499$. Therefore, we see that among these 14 pairs, F does not satisfy (H'_p) except for the case where $(p, [F : \boldsymbol{Q}]) = (43, 2)$, $(67, 2)$ or $(163, 2)$. By [5, Remark 2], we already know that F satisfies (H'_p) when $(p, [F : \boldsymbol{Q}]) = (43, 2)$ or $(67, 2)$.

From the above, it suffices to deal with the case where $(p, [F : \boldsymbol{Q}]) = (163, 2)$. Let $p = 163$, $K = \boldsymbol{Q}(\zeta_p)$, and $F = \boldsymbol{Q}(\sqrt{-p})$. Let $G = \mathrm{Gal}(K/\boldsymbol{Q}) = (\boldsymbol{Z}/p)^\times$ and $H = \mathrm{Gal}(K/F) \subseteq G$. We prove that $\mathcal{S}_H$ kills Cl_K. Let $\theta_{r,H} = (\theta_r)_H \in \mathcal{S}_H$ be the H-part of the Stickelberger element θ_r in the sense of (1). Letting $J = \sigma_{-1}$ be the complex conjugation, we see that $G = H \cdot \langle J \rangle$ and $(1 - J)\boldsymbol{Z}[G] = (1 - J)\boldsymbol{Z}[H]$. As is well known, the Stickelberger elements of $\boldsymbol{Z}[G]$ live essentially in the odd part $(1 - J)\boldsymbol{Z}[G]$. This fact is expressed in the form

$$\theta_r = (1 - J)\theta_{r,H} + (r - \delta_r) J N_H$$

for each $r \in \boldsymbol{Z}$. Here, N_H is the norm element of $\boldsymbol{Z}[H]$, and $\delta_r = 0$ or 1 according to whether p divides r or not. For this formula, see [4, Lemma 1]. By the classical Stickelberger theorem, θ_r kills Cl_K. Further, the norm N_H kills Cl_K as $h_F = 1$. Hence, we see that $(1 - J)\theta_{r,H}$ kills Cl_K. On the other hand, it is known that $h_p^+ = 4$ under GRH by van der Linden [7] and $h_p^- = 4 \cdot N$ for some odd integer N. Therefore, it follows that $\theta_{r,H}$ kills the q-part $Cl_K(q)$ for any odd prime number q (under GRH). Now, it suffices to show that $\mathcal{S}_H$ kills the 2-part $Cl_K(2)$. Let E

be the intermediate field of K/F with $[E : F] = 3$, and let $\Delta = \mathrm{Gal}(E/F)$. We have $h_{E^+} = 4$ by Uchida [11] and $h_E^- = 4$ by [8, Table 1]. In particular, as $[K : E]$ is odd, the natural map $Cl_E \to Cl_K(2)$ is an isomorphism (under GRH). Let φ be the restriction map $\boldsymbol{Z}[H] \to \boldsymbol{Z}[\Delta]$, and put $\bar{\mathcal{S}}_H = \varphi(\mathcal{S}_H)$ and $\bar{\theta}_{r,H} = \varphi(\theta_{r,H})$. From the above, $\mathcal{S}_H$ kills $Cl_K(2)$ if and only if $\bar{\mathcal{S}}_H$ kills Cl_E. Using a group theoretical argument in Iwasawa [6], we can show that Cl_{E^+} and Cl_E^- are both isomorphic to $(\boldsymbol{Z}/2)^{\oplus 2}$, and that Cl_E is isomorphic to $(\boldsymbol{Z}/2)^{\oplus 4}$ or $(\boldsymbol{Z}/4)^{\oplus 2}$. Hiroki Sumida-Takahashi calculated that

$$Cl_E \cong (\boldsymbol{Z}/2)^{\oplus 4} \tag{5}$$

using KASH. As $G = \langle \sigma_2 \rangle$ and $H = \langle \sigma_4 \rangle$, we see from (2) that $\mathcal{S}_{H,2}$ is generated by $\theta_{2,H}$ and $\theta_{4,H}$ over $\boldsymbol{Z}_2[H]$. Therefore, for showing $Cl_K(2)^{\mathcal{S}_H} = \{0\}$, it suffices to show that the elements $\bar{\theta}_{2,H}$ and $\bar{\theta}_{4,H}$ kill Cl_E. Let $\rho = \varphi(\sigma_4)$. From the definition, we can easily calculate that

$$\bar{\theta}_{2,H} = 13 + 11\rho + 15\rho^2 \equiv 1 + \rho + \rho^2 \ (= N_{E/F}) \mod 2$$

and

$$\bar{\theta}_{4,H} = 42 + 34\rho + 44\rho^2 \equiv 0 \mod 2.$$

Therefore, by (5) and $h_F = 1$, we see that $\bar{\mathcal{S}}_H$ kills Cl_E. Now, from the above, we can conclude that $F = \boldsymbol{Q}(\sqrt{-p})$ satisfies (H'_p) for $p = 163$ under GRH.

Acknowledgments

The author thanks the referee for valuable comments which improved the presentation of the whole paper. The author thanks H. Sumida-Takahashi for the information on the class group of the sextic abelian field of conductor 163. He is grateful to K. Yamamura for sending him the huge table [13] on h_p^-. The author was partially supported by Grant-in-Aid for Scientific Research (C) (No. 19540005), Japan Society for the Promotion of Science.

References

[1] K. Horie, On the class numbers of cyclotomic fields, Manuscripta Math. 65 (1989) 465–477.
[2] H. Ichimura, On a theorem of Kawamoto on normal bases of rings of integers, II, Canad. Math. Bull. 48 (2005) 576–579.
[3] H. Ichimura, Stickelberger ideals and normal bases of rings of p-integers, Math. J. Okayama Univ. 48 (2006) 9–20.
[4] H. Ichimura, A class number formula for the p-cyclotomic field, Arch. Math. (Basel) 87 (2006) 539–545.
[5] H. Ichimura, H. Sumida-Takahashi, Stickelberger ideals of conductor p and their application, J. Math. Soc. Japan 58 (2006) 885–902.
[6] K. Iwasawa, A note on ideal class groups, Nagoya Math. J. 27 (1966) 239–247.
[7] F.J. van der Linden, Class number computations of real abelian number fields, Math. Comp. 39 (1982) 693–707.
[8] S. Louboutin, Determination of all imaginary abelian number fields with relative class numbers any 2 power, which are composita of imaginary abelian number fields with prime power conductors, in: Number Theory, Liptovský, 1995, Tatra Mt. Math. Publ. 11 (1997) 43–58.
[9] B. Mazur, A. Wiles, Class fields of abelian extensions of $\boldsymbol{Q}$, Invent. Math. 76 (1984) 179–330.
[10] L.R. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra 82 (1983) 102–134.
[11] K. Uchida, On a cubic cyclic field with discriminant 163^2, J. Number Theory 8 (1976) 346–349.
[12] L.C. Washington, Introduction to Cyclotomic Fields, second ed., Springer, New York, 1997.
[13] K. Yamamura, Table of relative class numbers of imaginary abelian number fields of prime power conductors $\leqslant 2^{10} = 1024$, available at: ftp://tnt.math.metro-u.ac.jp/pub/table/rcn/.